Discrete Mathematics 118 (1993) 207–223
North-Holland

Codes for perfectly correcting errors of limited size

Samira Saidi

Department of Mathematics, University of Bahrain, P.O. Box 32038, Bahrain

Received 13 February 1990
Revised 18 October 1991

Abstract

Saidi S., Codes for perfectly correcting errors of limited size, Discrete Mathematics 118 (1993) 207–223.

In this paper we study an analogue of perfect codes: codes that perfectly correct errors of limited size, assuming that there is a bound on the number of these errors.

1. Introduction

Let Z_s be the ring of integers mod s represented by the complete system of residues $(-s/2, s/2]$, and let e and m be positive integers. A generalized cross (or semicross) over this s-letter alphabet $\mathscr{A}=Z_s$ $(s\geqslant 2m+1)$ is any translate of the unit cubes centered at the elements of the following set:

$$B_{e,m}(0)=\{y\in\mathscr{A}^n \mid w_H(y)\leqslant e,\ 0\leqslant|y_i|\leqslant m,\ 1\leqslant i\leqslant n\} \quad \text{(cross)},$$

$$\tilde{B}_{e,m}(0)=\{y\in\mathscr{A}^n \mid w_H(y)\leqslant e,\ 0\leqslant y_i\leqslant m,\ 1\leqslant m,\ 1\leqslant i\leqslant n\} \quad \text{(semicross)}.$$

Here $w_H(x)=|\{1\leqslant i\leqslant n \mid x_i\neq 0\}|$, for $(x_1,\ldots,x_n)\in\mathscr{A}^n$.

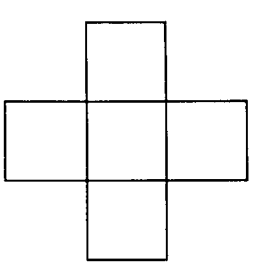
Figures 1 and 2 represent, respectively, generalized crosses and semicrosses in dimensions 2 and 3.

In this paper we treat the problem of tiling (disjoint covering) $\mathscr{A}^n$ $(\mathscr{A}=Z_s)$ by generalized crosses and semicrosses. A perfect, e,m code is by definition the set of the centers of the generalized crosses (or semicrosses) in such a tiling. Necessary and/or sufficient conditions for the existence of perfect codes in each case are presented along with some applications.

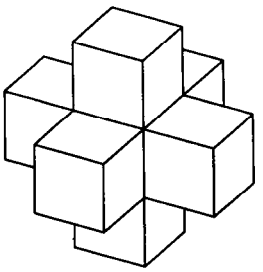
Translates of the unit cubes centered at the elements of $B_{1,m}(0)$ (or $\tilde{B}_{1,m}(0)$) are Stein's (m,n) crosses (or (m,n) semicrosses) [4, 5].

Correspondence to: Samira Saidi, Department of Mathematics, University of Bahrain, P.O. Box 32038, Isa Town, Bahrain.

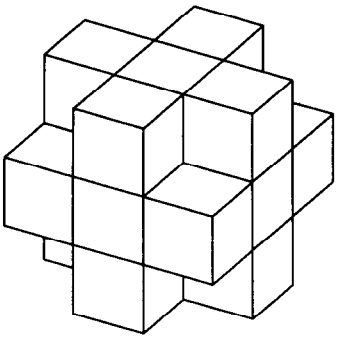
0012-365X/93/$06.00



$e=1,\ m=1,\ n=2$

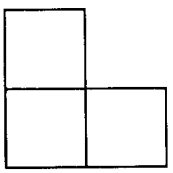


$e=1,\ m=1,\ n=3$

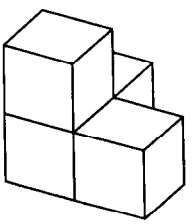


$e=2,\ m=1,\ n=3$

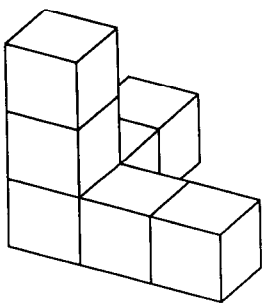
Fig. 1.



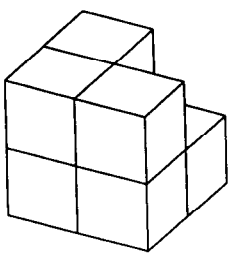
$e=1,\ m=1,\ n=2$



$e=1,\ m=1,\ n=3$



$e=1,\ m=2,\ n=3$



$e=2,\ m=1,\ n=3$

Fig. 2.

2. Conditions for the existence of tilings by generalized crosses

Theorem 2.1 (The sphere packing condition). *If a perfect e,m code $\mathscr{C} \subset \mathscr{A}^n$ exists, then*

$$|\mathscr{C}| \sum_{i=0}^{e} \binom{n}{i} (2m)^i = s^n$$

where $|\mathscr{C}|$ denotes the size of $\mathscr{C}$.

Proof. If $\mathscr{C} \subset \mathscr{A}^n$ is a perfect e,m code, we have $\bigsqcup_{x \in \mathscr{C}} B_{e,m}(x) = \mathscr{A}^n$ (where $\bigsqcup$ denotes a disjoint union), and

$$|B_{e,m}(0)| = \sum_{i=0}^{e} \binom{n}{i} (2m)^i.$$

The theorem follows at once from this. □

Lloyd's theorem (a necessary condition for the existence of perfect codes in the Hamming case) has been extended to the Lee metric by Bassalygo [1]. In the following, using a similar idea we extend it to generalized crosses.

Definition. For $a \in \mathscr{A}^n$, its composition vector and composition function are respectively defined by

$$c(a) = \begin{cases} (c_{-s'+1}(a), \ldots, c_{-1}(a), c_1(a), \ldots, c_{s'}(a)) & \text{if } s \text{ is even,} \\ (c_{-s'}(a), \ldots, c_{-1}(a), c_1(a), \ldots, c_{s'}(a)) & \text{if } s \text{ is odd,} \end{cases}$$

$$X^{c(a)} = \begin{cases} x_1^{c_{-s'+1}(a)} \cdots x_{s'-1}^{c_{-1}(a)} x_{s'}^{c_1(a)} \cdots x_{s-1}^{c_{s'}(a)} & \text{if } s \text{ is even,} \\ x_1^{c_{-s'}(a)} \cdots x_{s'-1}^{c_{-1}(a)} x_{s'+1}^{c_1(a)} \cdots x_{s-1}^{c_{s'}(a)} & \text{if } s \text{ is odd,} \end{cases}$$

where $s' = [s/2]$ and $c_i(a)$ is the number of coordinates of a equal to i ($c_i(a) \leqslant n$).

In the following we assume s to be odd, so $s' = (s-1)/2$; the case of s even goes in a similar way.

Definition. If $\mathscr{C} \subset \mathscr{A}^n$, its composition function is defined by the following polynomial in $s-1$ variables:

$$\Phi_{\mathscr{C}}(x_1, \ldots, x_{s-1}) = \sum_{a \in \mathscr{C}} x_1^{c_{-s'}(a)} \cdots x_{s'}^{c_{-1}(a)} x_{s'+1}^{c_1(a)} \cdots x_{s-1}^{c_{s'}(a)}.$$

Note. If $\mathscr{C} \subset \mathscr{A}^n$ is a perfect e,m code then $a + \mathscr{C}$, $a \in \mathscr{A}^n$, is a perfect e,m code (since generalized crosses are invariant under translation). Hence, we may assume that $0 \in \mathscr{C}$.

Lemma 2.2. *Let $A \subset B_{e,m}(0)$ be such that all its elements have distinct composition vectors, and let $\mathscr{C} \subset \mathscr{A}^n$ be a perfect e,m code. Then*

$$\forall a \in A \ \exists v_0 \in \mathscr{C}, \qquad \forall b \in A,\ b \neq a,\ c(a + v_0) \neq c(b + v).$$

Proof (*by contradiction*). Let $a \in A$ be such that there exists v in $\mathscr{C}$ and b in A, $b \neq a$, satisfying $c(a) = c(b+v)$. We have $v \neq 0$ since otherwise we get $c(a) = c(b)$ contradicting the assumption on A. We also have $w_H(a) = w_H(b+v)$ $(w_H(a) = \sum_{i=1}^{s'} (c_i(a) + c_{-i}(a)))$ and $|b_i + v_i| \leqslant m \ \forall 1 \leqslant i \leqslant n$ (since $b + v = \pi_n(a)$ for some permutation π_n of order n, and $a \in A \subset B_{e,m}(0)$). Therefore $b + v \in B_{e,m}(0)$, but $b + v \in B_{e,m}(v)$ (since $b \in B_{e,m}(0)$); this contradicts the disjointness of $B_{e,m}(0)$ and $B_{e,m}(v)$. □

Proposition 2.3. *Let A be the largest subset of $B_{e,m}(0)$ all of whose elements have distinct composition vectors. Then $|A| = \binom{2m+e}{2m}$.*

Proof. For $y \in \mathscr{A}^n$ we have

$$w_H(y) = \sum_{i=1}^{s'} (c_i(y) + c_{-i}(y)).$$

Hence,

$$B_{e,m}(0) = \left\{ y \in \mathscr{A}^n \mid \sum_{i=1}^{s'} (c_i(y) + c_{-i}(y)) \leqslant e, \ |y_i| \leqslant m \ \forall 1 \leqslant i \leqslant n \right\},$$

i.e.

$$B_{e,m}(0) = \left\{ y \in \mathscr{A}^n \mid \sum_{i=1}^{s'} (c_i(y) + c_{-i}(y)) \leqslant e, \right.$$

$$\left. c_i(y) = 0 = c_{-i}(y) = 0 = c_{-i}(y) \ \forall m+1 \leqslant i \leqslant s' \right\}.$$

A is thus formed by all such elements with distinct composition vectors, and $|A|$ is equal to the number of all distinct ordered $2m$-tuples of nonnegative integers $(u_1, \ldots, u_{2m})$ such that $u_1 + u_2 + \cdots + u_{2m} \leqslant e$, i.e. $\binom{2m+e}{2m}$. □

Definition. On the space of polynomials in $s-1$ variables of degree $\leqslant n$ with complex coefficients, define the linear map $M_{e,m}$ by

$$M_{e,m}(X^{c(a)}) = \sum_{b \in B_{e,m}(0)} X^{c(a+b)}, \quad a \in \mathscr{A}^n.$$

$M_{e,m}$ transforms the composition function of any point $a \in \mathscr{A}^n$ into the composition function of the generalized cross centered at a. It is uniquely defined because the composition functions of two generalized crosses are equal if the composition function of their centers are; and all distinct composition functions of points form a basis of the space of polynomials of degree $\leqslant n$ in $s-1$ variables.

Lemma 2.4. *If $\mathscr{C} \subset \mathscr{A}^n$ is a perfect e, m code, then*

$$M_{e,m} \Phi_{\mathscr{C}}(x_1, \ldots, x_{s-1}) = \Phi_{\mathscr{A}^n}(x_1, \ldots, x_{s-1}).$$

Proof. $\mathscr{C}$ being a perfect e,m *code, we have*

$$\bigsqcup_{x\in\mathscr{C}} B_{e,m}(x)=\mathscr{A}^n.$$

Hence,

$$M_{e,m}(x_1,\ldots,x_{s-1})=\sum_{a\in\mathscr{C}}\sum_{b\in B_{e,m}(0)} X^{c(a+b)}=\sum_{a\in\mathscr{C}}\sum_{b\in B_{e,m}(a)} X^{c(b)}$$

$$=\sum_{b\in\bigsqcup_{a\in\mathscr{C}} B_{e,m}(a)} X^{c(b)}=\Phi_{\mathscr{A}^n}(x_1,\ldots,x_{s-1}). \qquad \square$$

Proposition 2.5. *If a perfect* e,m *code* $\mathscr{C}\subset\mathscr{A}^n$ *exists then the nullity of the linear map* $M_{e,m}$ *(i.e. the number of linearly independent eigenfunctions with eigenvalue* 0*) is at least* $\binom{2m+e}{2m}-1$.

Proof. Let A be as in Proposition 2.3. Then $\Phi_{a+\mathscr{C}}(x_1,\ldots,x_{s-1})$, $a\in A$, are linearly independent (this follows from Lemma 2.2), and we have

$$M_{e,m}(\Phi_{a+\mathscr{C}}(x_1,\ldots,x_{s-1})-\Phi_{\mathscr{C}}(x_1,\ldots,x_{s-1}))=0 \quad \text{(by Lemma 2.4).}$$

The proposition then follows. $\square$

Let $\chi_a(d)$, $a,d\in\mathscr{A}^n$, be the complex characters of $\mathscr{A}^n$ defined by

$$\chi_a(d)=e^{(2\pi i/s)\sum_{j=1}^{n} a_j d_j},$$

and let

$$f_a(x_1,\ldots,x_{s-1})=\sum_{d\in\mathscr{A}^n}\chi_a(d)X^{c(d)}.$$

Lemma 2.6. f_a *is an eigenfunction of* $M_{e,m}$ *with eigenvalue equal to the sum of its coefficients for all monomials* $x_1^{r_1}x_2^{r_2}\cdots x_{s-1}^{r_{s-1}}$ *such that*

$$\sum_{i=1}^{s-1} r_i\leqslant e \quad \text{and} \quad r_{m+1}=\cdots=r_{s-m+1}=0.$$

Proof.

$$M_{e,m}f_a(x_1,\ldots,x_{s-1})$$

$$=\sum_{b\in B_{e,m}(0)}\sum_{d\in\mathscr{A}^n}\chi_a(d)x_1^{c_{-s'}(d+b)}\cdots x_{s'-1}^{c_{-1}(d+b)}x_{s'+1}^{c_1(d+b)}\cdots x_{s-1}^{c_{s'}(d+b)}$$

$$=\sum_{b\in B_{e,m}(0)}\sum_{d\in\mathscr{A}^n}\chi_a(d-b)x_1^{c_{-s'}(d)}\cdots x_{s'-1}^{c_{-1}(d)}x_{s'+1}^{c_1(d)}\cdots x_{s-1}^{c_{s'}(d)}$$

$$=\left(\sum_{b\in B_{e,m}(0)}\chi_a(-b)\right)\sum_{d\in\mathscr{A}^n}\chi_a(d)x_1^{c_{-s'}(d)}\cdots x_{s'-1}^{c_{-1}(d)}x_{s'+1}^{c_1(d)}\cdots x_{s-1}^{c_{s'}(d)}.$$

But $b\in B_{e,m}(0)$ iff $-b\in B_{e,m}(0)$. Hence,

$$M_{e,m}f_a(x_1,\ldots,x_{s-1})=\Bigg(\sum_{b\in B_{e,m}(0)}\chi_a(b)\Bigg)f_a(x_1,\ldots,x_{s-1}),$$

and, since

$$B_{e,m}(0)=\Bigg\{y\in\mathscr{A}^n\,|\,\sum_{i=1}^{n}(c_i(y)+c_{-i}(y))\leqslant e;\ c_i(y)=0=c_{-i}(y)\text{ for } m+1\leqslant i\leqslant s'\Bigg\},$$

the lemma follows by letting $(r_1,\ldots,r_{s-1})=(c_{-s'}(d),\ldots,c_{-1}(d),c_1(d),\ldots,c_{s'}(d))$ in the expression for f_a. □

By induction on n, we prove the following lemma.

Lemma 2.7.

$$f_a(x_1,\ldots,x_{s-1})=\prod_{k=-s'}^{s'}\Bigg(1+\sum_{l=1}^{s-1}\mathrm{e}^{(2\pi\mathrm{i}/s)kl}z_l\Bigg)^{c_k(a)},$$

where

$$c_0(a)=n-(c_{-s'}(a)+\cdots+c_{-1}(a)+c_1(a)+\cdots+c_{s'}(a))$$

and

$$z_l=\begin{cases}x_{l+s'}, & 1\leqslant l\leqslant s',\\ x_{l-s'}, & s'+1\leqslant l\leqslant s-1.\end{cases}$$

Note.

$$c_0(a)=\begin{cases}1 & \text{if } a=(0,\ldots,0),\\ 0 & \text{otherwise.}\end{cases}$$

Proposition 2.8. *The functions* $\Psi_{u_1\cdots u_{s-1}}(z_1,\ldots,z_{s-1})$ *defined by*

$$\Psi_{u_1\cdots u_{s-1}}(z_1,\ldots,z_{s-1})=\prod_{k=0}^{s-1}\Bigg(1+\sum_{l=1}^{s-1}\mathrm{e}^{(2\pi\mathrm{i}/s)kl}z_l\Bigg)^{u_k}$$
$$=\sum_{r_1+\cdots+r_{s-1}\leqslant n}\Psi^{r_1\ldots r_{s-1}}_{u_1\ldots u_{s-1}}z_1^{r_1}\cdots z_{s-1}^{r_{s-1}},$$

where u_k, $0\leqslant k\leqslant s-1$, *are nonnegative integers with sum n, form a complete system of eigenfunctions of* $M_{e,m}$, *and*

$$M_{e,m}\Psi_{u_1\ldots u_{s-1}}(z_1,\ldots,z_{s-1})$$
$$=\Bigg(\sum_{\substack{r_1+\cdots+r_{s-1}\leqslant e\\ r_{m+1}=\cdots=r_{s-m-1}=0}}\Psi^{r_1\ldots r_{s-1}}_{u_1\ldots u_{s-1}}\Bigg)\Psi_{u_1\ldots u_{s-1}}(z_1,\ldots,z_{s-1}).$$

Proof. The $f_a(x_1, \ldots, x_{s-1})$, a running through a subset of $\mathscr{A}^n$ all of whose elements have distinct composition vectors, are linearly independent [1]. The proposition then follows from Lemmas 2.6 and 2.7 by letting

$$(u_1, \ldots, u_{s-1}) = (c_{-s'}(a), \ldots, c_{-1}(a), c_1(a), \ldots, c_{s'}(a))$$

and using the fact that the number of these f_a's is $\binom{n+s+1}{s-1}$, which is the dimension of the space of polynomials in $s-1$ variables of degree $\leqslant n$. □

Proposition 2.8 is established similarly for s even; we then have the following theorem for any s.

Theorem 2.9 (An analogue of Lloyd's theorem). *If a perfect e,m code $\mathscr{C} \subset \mathscr{A}^n$ exists, then there are at least $\binom{2m+e}{2m}-1$ distinct $(s-1)$-tuples of nonnegative integers $(u_1, \ldots, u_{s-1})$ such that $u_0+u_1+\cdots+u_{s-1}=n$ and the sum of the coefficients of $z_1^{r_1}, \ldots, z_{s-1}^{r_{s-1}}, r_1+\cdots+r_{s-1} \leqslant e$, $r_{m+1}=\cdots=r_{s-m-1}=0$ in the product*

$$\prod_{k=0}^{s-1} \left(1+\sum_{l=1}^{s-1} e^{(2\pi i/s)kl} z_l\right)^{u_k}$$

is zero.

Theorem 2.10 (A sufficient condition for a perfect e,m code). *If*

$$s=\sum_{r=0}^{e} \binom{n}{r} (2m)^r$$

and there is a set $I=\{i_1, \ldots, i_n\}$ of n integers in $[1,(s-1)/2]$ such that $S_0=0$ and the sums

$$S_k=\sum_{j=1}^{k} \alpha_j i_j \ (1 \leqslant k \leqslant e), \quad \alpha_j \text{ integers with } 1 \leqslant |\alpha_j| \leqslant m,\ i_j \in I,\ i_j\text{'s distinct}$$

are incongruent mod s, *then a perfect e,m code exists, given by*

$$\mathscr{C}=\left\{x \in \mathscr{A}^n \mid \sum_{k=1}^{n} i_k x_k \equiv 0 \pmod{s}\right\}.$$

Note. The number of sums S_k, $0 \leqslant k \leqslant e$, is exactly s.

Proof. Let $x \neq 0$ in $\mathscr{C}$. We need only show that $B_{e,m}(0) \cap B_{e,m}(x) = \emptyset$, since

$$|\mathscr{C} \| B_{e,m}(0)| = s^{n-1} \sum_{i=0}^{e} \binom{n}{i} (2m)^i = s^n.$$

If there is $y=(y_1, \ldots, y_n) \in B_{e,m}(0) \cap B_{e,m}(x)$ then $y_i \in [-m,m]$, $y_i=0$ for all but at most e i's, and $y=x+z$, where $z_i \in [-m,m]$ and $z_i=0$ for all but at most e i's. We have

$$\sum_{k=1}^{n} y_k i_k = \sum_{k=1}^{n} x_k i_k + \sum_{k=1}^{n} z_k i_k \quad (y \neq z).$$

Hence,

$$\sum_{k=1}^{n} y_k i_k \equiv \sum_{k=1}^{n} z_k i_k \pmod{s},$$

contradicting the assumption on the set I and proving the theorem. □

3. Applications

In the following ζ denotes a primitive sth root of unity.

Definition. We define the trace map (denoted by tr) in $Q(\zeta)$ as in algebraic number theory; see, for example, [3]. We note in particular that

(1) for $s=p^\alpha$, $\alpha \geqslant 1$, $\operatorname{tr}(\zeta^k)=\begin{cases} p^{\alpha-1}(p-1) & \text{if } \zeta^k=1, \\ -p^{\alpha-1} & \text{if } \zeta^k \text{ is a } p\text{th root of unity}, \\ 0 & \text{otherwise}, \end{cases}$

(2) for $s=p^\alpha q^\beta$, $\alpha, \beta \geqslant 1$, $\operatorname{tr}(\zeta^k)=$

$$\begin{cases} p^{\alpha-1}q^{\beta-1}(p-1)(q-1) & \text{if } \zeta^k=1, \\ p^{\alpha-1}q^{\beta-1} & \text{if } \zeta^k \text{ is a } pq\text{th root of unity}, \\ -p^{\alpha-1}q^{\beta-1}(q-1) & \text{if } \zeta^k \text{ is a } p\text{th root of unity}, \\ -p^{\alpha-1}q^{\beta-1}(p-1) & \text{if } \zeta^k \text{ is a } q\text{th root of unity}, \\ 0 & \text{otherwise.} \end{cases}$$

Proposition 3.1. *If $s=p^\alpha-1+2mn$, $\alpha>1$ (p prime), $1<m<p$ and $p-1 \not\equiv 0 \pmod{2m}$, then there is no perfect $1,m$ code.*

Proof. From Theorem 2.9 we know that if a perfect $1,m$ code exists, then there are at least $2m$ distinct $(s-1)$-tuples of nonnegative integers $(u_1, \ldots, u_{s-1})$ such that $u_0+u_1+\cdots+u_{s-1}=n$ and such that the sum of the constant term and the coefficients of $z_1, z_2, \ldots, z_m, z_{s-m}, \ldots, z_{s-2}\, z_{s-1}$ in

$$\prod_{k=0}^{s-1}\left(1+\sum_{l=1}^{s-1}\zeta^{kl}z_l\right)^{u_k}$$

is zero.

Computing this sum, we get

$$1+2mu_0+\sum_{i=1}^{(s-1)/2}(u_i+u_{s-i})(\zeta^i+\zeta^{2i}+\cdots+\zeta^{mi}+\zeta^{-mi}+\cdots+\zeta^{-2i}+\zeta^{-i})=0, \tag{3.1}$$

that is,

$$p^\alpha+\sum_{i=1}^{(s-1)/2}(u_i+u_{s-i})(\zeta^i+\zeta^{2i}+\cdots+\zeta^{mi}+\zeta^{-mi}+\cdots+\zeta^{-2i}+\zeta^{-i}-2m)=0.$$

Thus,

$$p^\alpha+\sum_{\substack{(i,p)=1\\1\leqslant i\leqslant(s-1)/2}}(u_i+u_{s-i})(\zeta^i+\cdots+\zeta^{mi}+\zeta^{-mi}+\cdots+\zeta^{-i}-2m)$$
$$+\sum_{\substack{i\equiv 0\,(p^{\alpha-1})\\1\leqslant i\leqslant(s-1)/2}}(u_i+u_{s-i})(\zeta^i+\cdots+\zeta^{mi}+\zeta^{-mi}+\cdots+\zeta^{-i}-2m)$$
$$+\sum_{\substack{i\equiv 0\,(p^\beta),\,\beta<\alpha-1\\i\not\equiv 0\,(p^{\beta+1})\\1\leqslant i\leqslant(s-1)/2}}(u_i+u_{s-i})(\zeta^i+\cdots+\zeta^{mi}+\zeta^{-mi}+\cdots+\zeta^{-i}-2m)=0,$$

where (i,p) denotes the g.c.d. of i and p. Then taking the trace, we get (since $m<p$)

$$p^\alpha p^{\alpha-1}(p-1)+\sum_{(i,p)=1}(u_i+u_{s-i})[-2mp^{\alpha-1}(p-1)]$$
$$+\sum_{i\equiv 0\,(p^\alpha-1)}(u_i+u_{s-i})[-2mp^{\alpha-1}-2mp^{\alpha-1}(p-1)]$$
$$+\sum_{\substack{i\equiv 0\,(p^\beta),\,\beta<\alpha-1\\i\not\equiv 0\,(p^{\beta+1})}}(u_i+u_{s-i})[-2mp^{\alpha-1}(p-1)]=0,$$

which is impossible by congruence modulo $2m$. This finishes the proof. □

Proposition 3.2. *If $s=p^\alpha q^\beta=1+2mn$, $\alpha\geqslant 1$, $\beta\geqslant 1$, where p and q are primes such that $2<m<p$, $m<q$ and $(p-1)(q-1)\not\equiv 0\,(\mathrm{mod}\,2m)$, then there is no perfect $1,m$ code.*

Proof. The idea is similar to the proof of Proposition 3.1. In (3.1), let $A_{i,m,s}=(u_i+u_{s-i})(\zeta^i+\cdots+\zeta^{mi}+\zeta^{-mi}+\cdots+\zeta^{-i}-2m)$. Let J be the set of integers in $[1,(s-1)/2]$ and I the set of i's in J satisfying

$$\begin{cases} i\equiv 0(p^{\alpha-1}q^{\beta-1})\\ i\not\equiv 0(p^\alpha)\\ i\not\equiv 0(q^\beta), \end{cases} \qquad \begin{cases} i\equiv 0(p^{\alpha-1})\\ i\not\equiv 0(p^\alpha)\\ i\equiv 0(q^\beta), \end{cases} \quad \text{or} \quad \begin{cases} i\equiv 0(q^{\beta-1})\\ i\not\equiv 0(q^\beta)\\ i\equiv 0(p^\alpha). \end{cases}$$

We get

$$p^\alpha q^\beta+\sum_{\substack{i\equiv 0\,(p^{\alpha-1}q^{\beta-1})\\i\not\equiv 0(p^\alpha)\\i\not\equiv 0(q^\beta)\\i\in J}}A_{i,m,s}+\sum_{\substack{i\equiv 0\,(p^{\alpha-1})\\i\not\equiv 0\,(p^\alpha)\\i\equiv 0\,(q^\beta)\\i\in J}}A_{i,m,s}+\sum_{\substack{i\equiv 0\,(q^{\beta-1})\\i\not\equiv 0\,(q^\beta)\\i\equiv 0\,(p^\alpha)\\i\in J}}A_{i,m,s}+\sum_{i\in J\setminus I}A_{i,m,s}=0.$$

(Note that $J\backslash I=\emptyset$ in the case $\alpha=\beta=1$). Then taking the trace, we get (since $m<p$ and $m<q$)

$$
\begin{aligned}
& p^{\alpha}q^{\beta}p^{\alpha-1}q^{\beta-1}(p-1)(q-1) \\
& + \sum_{\substack{i=0\,(p^{\alpha-1}q^{\beta-1}) \\ i\neq 0\,(p^{\alpha}) \\ i\neq 0\,(q^{\beta}) \\ i\in J}} (u_i+u_{s-i})[2mp^{\alpha-1}q^{\beta-1}-2mp^{\alpha-1}q^{\beta-1}(p-1)(q-1)] \\
& + \sum_{\substack{i\equiv 0\,(p^{\alpha-1}) \\ i\neq 0\,(p^{\alpha}) \\ i\equiv 0\,(q^{\beta}) \\ i\in J}} (u_i+u_{s-i})[-2mp^{\alpha-1}q^{\beta-1}(q-1)-2mp^{\alpha-1}q^{\beta-1}(p-1)(q-1)] \\
& + \sum_{\substack{i\equiv 0\,(q^{\beta-1}) \\ i\neq 0\,(q^{\beta}) \\ i\equiv 0\,(p^{\alpha}) \\ i\in J}} (u_i+u_{s-i})[-2mp^{\alpha-1}q^{\beta-1}(p-1)-2mp^{\alpha-1}q^{\beta-1}(p-1)(q-1)] \\
& + \sum_{i\in J\setminus I} (u_i+u_{s-i})[-2mp^{\alpha-1}q^{\beta-1}(p-1)(q-1)]=0,
\end{aligned}
$$

This is impossible by congruence modulo $2m$; hence the proposition follows. □

Note. Proposition 3.2 can be generalized to the case $s=\prod_{i=1}^{r}p_i^{\alpha_i}=1+2mn, r>2$, $\alpha_i\geqslant 1$, $1\leqslant i\leqslant r$, assuming some restriction on the prime factors p_i, $1\leqslant i\leqslant r$.

From Theorem 2.9 we know that if a perfect e, m code exists, then the sum of the coefficients of $z_1^{r_1}, z_2^{r_2}, \ldots, z_{s-1}^{r_{s-1}}$, $r_1+r_2+\cdots+r_{s-1}\leqslant e$, $r_{m+1}=\cdots=r_{s-m+1}=0$ in the product

$$\prod_{k=0}^{s-1}\left(1+\sum_{l=1}^{s-1}\zeta^{kl}z_l\right)^{u_k},$$

is zero for at least $\binom{e+2m}{2m}-1$ s-tuples of nonnegative integers $(u_0, u_1, \ldots, u_{s-1})$ with sum n. Assuming that a perfect e, m code exists, let μ denote the number of nonzero u_i+u_{s-i}, $1\leqslant i\leqslant(s-1)/2$, in this sum.

Note. $\mu\leqslant n$.

Let $N(\mu)$ denote the number of distinct powers of ζ occurring in this sum (including the zero power). We have the following result.

Lemma 3.3. *If*

$$s=p=\sum_{i=0}^{e}\binom{n}{i}(2m)^i, \quad p \text{ prime},$$

then $\mu=n$.

Proof. Suppose $\mu \leqslant n-1$. We will show that $N(n-1)<p$, which implies that $N(\mu)<p \; \forall \mu \leqslant n-1$ (since $N(\mu)$ is an increasing function of μ). This contradicts the fact that the degree of the pth cyclotomic polynomial is $p-1$, and the lemma then follows from the above note. If $\mu = n-1$ then, since

$$\sum_{i=1}^{(p-1)/2} (u_i + u_{p-i}) \leqslant n,$$

we either have

$$\text{(i)} \quad \begin{cases} \sum\limits_{1 \leqslant i \leqslant (p-1)/2} (u_i + u_{p-i}) = n, \text{ in which case } u_0 = 0, \text{ and} \\ u_{i_1} + u_{p-i_1} = 2, \; u_{i_2} + u_{p-i_2} = \cdots = u_{i_{n-1}} + u_{p-i_{n-1}} = 1, \\ u_i + u_{p-i} = 0 \;\; \forall i \neq i_j, \; 1 \leqslant j \leqslant n-1, \text{ the } i_j\text{'s being distinct,} \end{cases}$$

or

$$\text{(ii)} \quad \begin{cases} \sum\limits_{1 \leqslant i \leqslant (p-1)/2} (u_i + u_{p-i}) = n, \text{ in which case } u_0 = 1, \text{ and} \\ u_{i_1} = u_{p-i_1} = \cdots = u_{i_{n-1}} + u_{p-i_{n-1}} = 1, \; u_i + u_{p-i} = 0, \\ \forall i \neq i_j, \; 1 \leqslant j \leqslant n-1, \text{ the } i_j\text{'s being distinct.} \end{cases}$$

Counting the number of power of ζ occurring, we see from the expression of the product that without loss of generality we can assume that $u_{i_1} = 2$, $u_{i_2} = \cdots = u_{i_{n-1}} = 1$ in case (i), and that $u_{i_1} = u_{i_2} = \cdots = u_{i_{n-1}} = 1$ in case (ii). Also from the expression of the product it is clear that the number of powers of ζ occurring in case (ii) is at most equal to the number of powers of ζ occurring in case (i). We can therefore consider only case (i), and the product becomes

$$\left(1 + \sum_{l=1}^{p-1} \zeta^{i_1 l} z_l\right)^2 \prod_{k=2}^{n-1} \left(1 + \sum_{l=1}^{p-1} \zeta^{i_k l} z_l\right)$$

Now we compute $N(n-1)$ from the product

$$\left(1 + \sum_{l=l}^{m} \zeta^{i_1 l} z_l + \sum_{l=s-m}^{s-1} \zeta^{i_1 l} z_l\right)^2 \prod_{k=2}^{n-1} \left(1 + \sum_{l=1}^{m} \zeta^{i_k l} z_l + \sum_{l=s-m}^{m} \zeta^{i_k l} z_l\right)$$

(refer to the definition of $N(n-1)$). Fix $1 \leqslant t \leqslant e$ and choose t factors of the n factors of this product. The number of powers of ζ occurring in the sum of the coefficients of $z_1^{r_1} z_2^{r_2} \cdots z_m^{r_m} z_{s-m}^{r_{s-m}} \cdots z_{s-1}^{r_{s-1}}$, $r_1 + \cdots + r_m + r_{s-m} + \cdots + r_{s-1} = t$ is $(2m)^t$ (clearly, not all of them are distinct). Hence,

$$N(n-1) < \sum_{t=0}^{e} \binom{n}{t} (2m)^t = p,$$

proving the lemma. □

Theorem 3.4. (A necessary and sufficient condition for the existence of a perfect e,m code). *If*

$$s=p=\sum_{r=0}^{e}\binom{n}{r}(2m)^r,$$

is prime, then a perfect e,m code exists if and only if there is a set I of n integers in $[1,(p-1)/2]$ such that 0 and the sums $\sum_{j=1}^{k}\alpha_j i_j$, $1\leqslant k\leqslant e$, α_j integers, with $1\leqslant|\alpha_j|\leqslant m$, and $i_j\in I$, i_j's distinct, are incongruent mod p.

Proof. The sufficiency is proved by Theorem 2.10. Now from Theorem 2.9 and Lemma 3.3 we know that if a perfect e,m code exists, then there is a set of n integers in $[1,(p-1)/2]$, $I=\{i_1,\ldots,i_n\}$, such that the sum of the constant term and the coefficients of

$$z_{\alpha_1},\ldots,z_{\alpha_{r_1}},z_{p-\alpha_{r_1+1}},\ldots,z_{p-\alpha_{r_1+r_2}},\quad 2\leqslant r_1+r_2\leqslant 2,\ r_1,r_2\geqslant 1,$$
$$1\leqslant\alpha_1\leqslant\cdots\leqslant\alpha_{r_1}\leqslant m,$$
$$1\leqslant\alpha_{r_1+1}\leqslant\cdots\leqslant\alpha_{r_1+r_2}\leqslant m$$

and

$$z_{\alpha_1},\ldots,z_{\alpha_r},\quad z_{p-\alpha_1},\ldots,z_{p-\alpha_r},\qquad 1\leqslant r\leqslant e,\ 1\leqslant\alpha_1\leqslant\cdots\leqslant\alpha_r\leqslant m$$

in

$$\prod_{j=1}^{n}\left(1+\sum_{l=1}^{p-1}\zeta^{i_j l}z_l\right)$$

is zero. Thus,

$$1+\sum_{\substack{1\leqslant a_1\leqslant\cdots\leqslant\alpha_r\leqslant m\\ 1\leqslant r\leqslant e\\ 1\leqslant k_1\neq\cdots\neq k_r\leqslant n}}(\zeta^{\alpha_1 i_{k_1}+\cdots+\alpha_r i_{k_r}}+\zeta^{-\alpha_1 i_{k_1}-\cdots-\alpha_r i_{k_r}})+$$
$$\sum_{\substack{1\leqslant\alpha_1\leqslant\cdots\leqslant\alpha_{r_1}\leqslant m\\ 1\leqslant\alpha_{r_1+1}\leqslant\cdots\leqslant\alpha_{r_1+r_2}\leqslant m\\ 2\leqslant r_1+r_2\leqslant e,\ r_1\geqslant 1\\ 1\leqslant k_1\neq\cdots\neq k_{r_1+r_2}\leqslant n}}\zeta^{\alpha_1 i_{k_1}+\cdots+\alpha_{r_1}i_{k_{r_1}}-\alpha_{r_1+1}i_{k_{r_1+1}}-\cdots-\alpha_{r_1+r_2}i_{k_{r_1+r_2}}i_{k_{r_1+r_2}}}=0. \tag{3.2}$$

But then the number of powers of ζ occurring in (3.2) is the number of powers of ζ in the sum of the coefficients of $z_1^{r_1}z_2^{r_2}\cdots z_m^{r_m}z_{s-m}^{r_{s-m}}\cdots z_{s-1}^{r_{s-1}}$,

$$r_1+\cdots+r_{s-1}\leqslant e,$$

computed from the product

$$\prod_{j=1}^{n}\left(1+\sum_{l=1}^{m}\zeta^{i_j l}z_l+\sum_{l=s-m}^{s-1}\zeta^{i_j l}z_l\right).$$

This number is clearly

$$\sum_{t=0}^{e} \binom{n}{t} (2m)^t = p$$

(refer to the proof of Lemma 3.3). Equation (3.2) is then true if and only if its left-hand side is $\Psi_p(\zeta)$, where Ψ_p is the pth cyclotomic polynomial; this proves the theorem. □

Examples. Let $PC(e, m, n)$ denote a perfect e, m code of length n over the alphabet of size

$$s = \sum_{i=0}^{e} \binom{n}{i} (2m)^i,$$

and let I be as in Theorem 3.4. We have:

$PC(1, 2, 3)$ exists if $s = p = 13$; $I = \{1, 3, 4\}$.

$PC\{1, 3, 23)$ exists if $s = p = 139$; a set I is given by the 6th powers mod 139;

$I = \{1, 6, 34, 36, 44, 45, 52, 55, 57, 63, 64, 65, 77, 79, 80, 91,$

$100, 106, 112, 116, 125, 129, 131\}$.

$PC(1, 2, 7)$ does not exist if $s = p = 29$.

$PC(2, 2, 3)$ does not exist if $s = p = 61$.

$PC(2, 1, 3)$ does not exist if $s = p = 19$ (a computer search shows that no set I can be found in these cases).

Definition. Let G be a finite abelian group, and $L = \{l_1, \ldots, l_k\}$ a set of k distinct integers. If there are elements $g_1, \ldots, g_n$ of G such that each nonzero element of G is uniquely expressible in the form $l_i g_j$, $1 \leqslant i \leqslant k$, $1 \leqslant j \leqslant n$, we say that L splits G.

Theorem 3.5 (Hamaker and Stein [2]). *Let G be a finite abelian group and $L = \{l_1, \ldots, l_k\}$ a set of integers, with each l_i relatively prime to $|G|$. Then L splits G iff L splits $C(p)$ for each prime divisor p of $|G|$, where $C(p)$ is the cyclic group of order p.*

Theorem 3.6 (Stein [5]). *A tiling of n-dimensional Euclidean space by (m, n) crosses (i.e. a perfect $1, m$ code) exists iff the set $\{\pm 1, \pm 2, \ldots, \pm m\}$ splits an abelian group G of order $1 + 2mn$.*

Lemma 3.7. *If $s = p = 1 + 2mn$, then a perfect $1, m$ code exists iff the set of integers in $[-m, m] - \{0\}$ splits $\mathscr{A}$.*

The proof follows from Theorem 3.4 (case $e = 1$).

Let Z_r denote the ring of integers mod r. We have the following result.

Proposition 3.8. *If $p^\alpha = 1 + 2mN$, $\alpha \geqslant 1$, and $p = 1 + 2mn$, p being a prime, then a perfect $1, m$ code of length N exists over Z_{p^α} iff a perfect $1, m$ code of length n exists over Z_p.*

The proof is an immediate consequence of Theorems 3.5 and 3.6 and Lemma 3.7.

Note. Proposition 3.1 states that if $s = p^\alpha = 1 + 2mn$, $\alpha \geqslant 1$, $m < p$ and $(p-1) \not\equiv 0 \pmod{2m}$, then there is no perfect $1, m$ code. Proposition 3.8 gives then a necessary and sufficient condition for the existence of perfect $1, m$ codes in the case $p = 1 \equiv 0 \pmod{2m}$.

Proposition 3.8 is generalized in the following theorem.

Theorem 3.9. *If $s = p_1^{\alpha_1} \cdots p_r^{\alpha_r} = 1 + 2mn$ is such that $p_i - 1 \equiv 0 \pmod{2m}$, $1 \leqslant i \leqslant r$, then a perfect $1, m$ code exists over Z_s iff a perfect $1, m$ code exists over Z_{p_i} $\forall 1 \leqslant i \leqslant r$.*

Note. Theorem 3.9 has been proved by Szabõ [6] for the case $m = 2$.

Examples.

$PC(1, 2, 42)$ exists if $s = 169$ (since $PC(1, 2, 3)$ exists if $s = p = 13$).

$PC(1, 2, 6)$ exists if $s = 25$ (since $PC(1, 2, 1)$ exists if $s = p = 5$).

$PC(1, 2, 210)$ does not exist if $s = 841$ (since $PC(1, 2, 7)$ does not exist if $s = p = 29$).

4. The case of generalized semicrosses

Recall that a perfect e, m code in this case is by definition the set of the centers of the generalized semicrosses in the tiling of $\mathscr{A}^n$.

Theorem 4.1 (The sphere packing condition). *If a perfect e, m code $\mathscr{C} \subset \mathscr{A}^n$ exists then*

$$|\mathscr{C}| \sum_{i=0}^{e} \binom{n}{i} m^i = s^n.$$

Proof. If $\mathscr{C} \subset \mathscr{A}^n$ is a perfect e, m code, then $\bigsqcup_{x \in \mathscr{C}} \tilde{B}_{e,m}(x) = \mathscr{A}^n$, and the theorem follows from

$$|\tilde{B}_{e,m}(0)| = \sum_{i=0}^{e} \binom{n}{i} m^i. \qquad \square$$

Analogous to the case of crosses, we establish the following results.

Theorem 4.2 (An analogue of Lloyd's theorem). *If a perfect e,m code $\mathscr{C} \subset \mathscr{A}^n$ exists, then there are at least $\binom{m+e}{m}-1$ $(s-1)$-tuples of nonnegative integers $(u_1,\ldots,u_{s-1})$ such that $u_0+u_1+\cdots+u_{s-1}=n$ and the sum of the coefficients of*

$$z_1^{r_1},\ldots,z_{s-1}^{r_{s-1}}, \quad r_1=\cdots=r_{s-m-1}=0,$$

in the product

$$\prod_{k=0}^{s-1}\left(1+\sum_{l=1}^{s-1} e^{(2\pi i/s)kl} z_l\right)^{u_k}$$

is zero.

Theorem 4.3 (A sufficient condition for a perfect e,m code). *If*

$$s=\sum_{r=0}^{e}\binom{n}{r}m^r$$

and there is a set I of n integers in $[1,s-1]$ such that 0 and the sums

$$\sum_{j=1}^{k}\alpha_j i_j \ (1\leqslant k\leqslant e), \quad \alpha_j \text{ integers, with } 1\leqslant\alpha_j\leqslant m,\ i_j\in I,\ i_j\text{'s distinct}$$

are incongruent mod s, *then a perfect e,m code exists, given by*

$$\mathscr{C}=\left\{x\in\mathscr{A}^n \sum_{k=1}^{n} i_k x_k\equiv 0 \pmod s\right\}.$$

Proposition 4.4. *If $s=2^n-1$, then a perfect $n-1,1$ code exists given by*

$$\mathscr{C}=\left\{x\in\mathscr{A}^n \mid \sum_{k=1}^{n} 2^{k-1}x_k\equiv 0 \pmod s\right\}.$$

The proof follows from Theorem 4.3 by letting $I=\{1,2,\ldots,2^{n-1}\}$.

We now state the following two propositions which are proved by the application of Theorem 4.2, and based on the idea used in the proofs of Propositions 3.1 and 3.2, respectively.

Proposition 4.5. *If $s=p^\alpha=1+mn$, $\alpha>1$, p prime, $m<n$ and $p-1\not\equiv 0 \pmod m$, then there is no perfect $1,m$ code.*

Proposition 4.6. *If $s=p^\alpha q^\beta=1+mn$, $\alpha\geqslant 1$, $\beta\geqslant 1$, $m\neq 2,\neq 4$, where p and q are primes such that $m<p$, $m<q$ and $(p-1)(q-1)\not\equiv 0 \pmod m$, then there is no perfect $1,m$ code.*

A necessary condition for the existence of a perfect e, m code is that the sum of the constant term and the coefficients of $z_{s-\alpha_1}, \ldots, z_{s-\alpha_r}$, $1 \leqslant r \leqslant e$, $1 \leqslant \alpha_1 \leqslant \cdots \leqslant \alpha_r \leqslant m$ in

$$\prod_{k=0}^{s-1} \left(1 + \sum_{l=1}^{s-1} \zeta^{kl} z_l\right)^{u_k}$$

is zero (Theorem 4.2).

Using this and proceeding similarly to the case of crosses, we prove that the necessary condition of Theorem 4.3 is also sufficient for the existence of a perfect e, m code in the case where the size of the alphabet

$$s = \sum_{i=0}^{e} \binom{n}{i} m^i$$

is a prime.

Examples. Let $PSC(e, m, n)$ denote a perfect e, m code of length n over the alphabet of size

$$s = \sum_{i=0}^{e} \binom{n}{i} m^i,$$

I as in Theorem 4.3. We have:

$PSC(1, 3, 2)$ exists if $s = p = 7$; $I = \{1, 6\}$.

$PSC(1, 3, 12)$ exists if $s = p = 37$; $I = \{1, 6, 8, 10, 11, 14, 23, 26, 27, 29, 31, 39\}$.

$PSC(4, 1, 5)$ exists if $s = p = 31$; $I = \{1, 2, 4, 8, 16\}$.

$PSC(2, 2, 3\}$ exists if $s = p = 19$; $I = \{1, 7, 11\}$.

$PSC(4, 2, 5)$ exists if $s = p = 211$; $I = \{1, 55, 71, 107, 188\}$ (I is the set of 42nd powers mod p).

$PSC(2, 1, 4)$ does not exist if $s = p = 11$.

$PSC(2, 1, 7)$ does not exist if $s = p = 29$ (by computer search).

$PSC(1, 3, 10)$ does not exist if $s = p = 31$ (by computer search).

Theorem 4.7 (Stein [5]). *A tiling of the n-dimensional Euclidean space by (m, n) semicrosses (i.e. a perfect $1, m$ code) exists iff the set $\{1, 2, \ldots, m\}$ splits an abelian group G of order $1 + mn$.*

Note. If $s = p = 1 + mn$, then a perfect $1, m$ code exists iff the set of integers in $[1, m]$ splits $\mathscr{A}$.

We give now the following results whose proofs are immediate consequences of Theorems 3.5, 4.3 (s being a prime) and 4.7 and the above note.

Proposition 4.8. *Let* $p^{\alpha}=1+mN$, $\alpha \geqslant 1$ *and* $p=1+mn$, p *prime. Then a perfect* $1,m$ *code of length* N *exists over* $Z_{p^{\alpha}}$ *iff a perfect* $1,m$ *code of length* n *exists over* Z_p.

Proposition 4.9. *If* $s=p_1^{\alpha_1}\cdots p_r^{\alpha_r}=1+mn$ *is such that* $p_i-1\equiv 0 \pmod{m}$, $1\leqslant i\leqslant r$, *then a perfect* $1,m$ *code exists over* Z_s *iff a perfect* $1,m$ *code exists over* Z_{p_i} $\forall 1\leqslant i\leqslant r$.

References

[1] L.A. Bassalygo, A necessary condition for the existence of perfect codes in the Lee metric, Math. Notes 15 (1974) 178–181.
[2] W. Hamaker and S. Stein, Splitting groups by integers, Proc. Amer. Math. Soc. 46 (1974).
[3] K. Ireland and M. Rosen, A classical introduction to modern number theory (Springer, New York, 1981).
[4] S. Stein, Factoring by subsets, Pac. J. Math. 22 (1967) 523–541.
[5] S. Stein, Algebraic tiling, Amer. Math. Monthly 31 (1974) 445–462.
[6] S. Szabò, On decomposing finite abelian groups, Acta Math. Acad. Scientiarum Hungaricae 36 (1980) 105–114.